REMARKS

These remarks follow the order of the paragraphs of the office action. Relevant portions of the office action are shown indented and italicized.

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statement (IDS) submitted on August 31, 2001 is in compliance with the provisions of 37 CFR 1:97. Accordingly, the information disclosure statement is being considered by the examiner.

Specification

2. The disclosure is objected to because of the following informalities: On page 1, line 10, application 09/240,503 is cross referenced and the status of the application should be updated to indicate that the application is now abandoned.
Appropriate correction is required.

In response, applicants respectfully state that the application is updates so that the words now abandoned were inserted into the specification. This overcomes the objection of the disclosure.

Claim Objections

3. Claims 10 are 18 are objected to because of the following informalities: On line 1 it is recited of "at least one table" that is a lack of antecedent basis. *It is unclear from the claim if the "table" is a "lookup table" or a "randomized table" as is claimed in claim 1. Appropriate correction is required.*

In response, applicants respectfully state that the words at "at least one table" is intended to mean **either** a "lookup table" or a "randomized table", **or both**. Thus there is indeed proper antecedent basis for the common word table as in claims 10 are 18.

Claim Rejections- USC § 102

4 The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:
A person shall be entitled to patent unless -

(b) the invention was patented or described in a printed publication in this or a foreign county or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-4, 10-13, 15, 18, 29, 30,36-43, 52,53.55 and 56 are rejected under 35 U.S.C. 102(b) as being anticipated by Chari et al. entitled "Towards Sound Approaches to Counteract Power-Analysis Attacks.

In response, applicants respectfully state that as stated in the abstract, the present invention as in claims 1-4, 10-13, 15, 18, 29, 30,36-43, 52,53.55 and 56 is for, "[M]ethods, apparatus and computer software and hardware products providing method, apparatus and system solutions for implementing table lookups in a side-channel attack resistant manner. Embodiments are provided for devices and situations where there is limited amount of RAM memory available or restrictions on memory addressing. The solutions solve problems associated with lookup tables with large indices, as well as problems associated with looking up large sized tables or a collection of tables of large cumulative size, in limited devices, in an efficient side-channel attack resistant manner. These solutions provide defenses against both first-order side channel attacks as well as higher-order side channel attacks. One aspect of the present invention is the creation of one or more random tables which are used possibly in conjunction with other tables to perform a table lookup. This denies an adversary information about the table lookup from the side channel and thereby imparting side-channel resistance to the table lookup operation. Another aspect of the present invention is the use of a combination of some operations such as Table Split, Table Mask and Table Aggregate, to achieve this side-channel resistance within the limited amounts of available RAM and limited memory addressing capabilities of the device performing table lookups." Thus claims 1-4, 10-13, 15, 18, 29, 30,36-43, 52,53.55 and 56 provides solutions and defenses against both first-order side channel attacks as well as higher-order side channel attacks.

Whereas the cited reference having three inventors common to the present application, Suresh Chari, Josyula R. Rao, and Pankaj Rohatgi provides, "[S]ide channel cryptanalysis techniques, such as the analysis of instantaneous power consumption, have been extremely effective in attacking implementations on simple hardware platforms. There are several proposed solutions to resist these attacks, most of which are ad-hoc and can easily be rendered ineffective. A scientific

approach is to create a model for the physical characteristics of the device, and then design implementations provably secure in that model. i.e., they resist generic attacks with an a priori bound on the number of experiments. We propose an abstract model which approximates power consumption in most devices and in particular small single-chip devices. Using this, we propose a generic technique to create provably resistant implementations for devices where the power model has reasonable properties, and a source of randomness exists. We prove a lower bound on the number of experiments required to mount statistical attacks on devices whose physical characteristics satisfy reasonable properties." This reference is thus not concerned with providing solutions and defenses against both first-order side channel attacks as well as higher-order side channel attacks.

As per claim 1, Chari et al discloses of a method comprising providing a data processing operation involving at least one lookup table, each particular table from said at least one lookup table having a particular lookup table size and a particular lookup table index size and creating at least one randomized table in which entries and/or indices are statistically independent from entries and/or indices of said at least one lookup table, each individual table from said at least one randomized table having a randomized table size, wherein a first sum of sizes of all said randomized tables is smaller than a second sum of sizes of all lookup tables, or the maximum index size of said randomized tables is less than the maximum index size of the lookup tables (see page 404, section 3.3).

In response, applicants respectfully state that in order to bring the application to allowance claim 1 is amended to include the limitation of objected-to claim 5. Claim 5 is canceled. This makes claim 1 and all claims 2- 18, 29, 30, 39, 40 and 53, that ultimately depend on claim 1 to be allowable.

As per claim 2, it is taught by Chari et al of using one randomized table (see page 404, section 3.3).

In response, applicants respectfully state that although applicants do not agree with the equivalencies made in the office action between claim 2 and the cited reference, they indicate that claim 2 is dependent on allowable claim 1 and is allowable.

As per claim 3, it is disclosed by Chari et al of obtaining data processing operations (see page 404, section 3.3).

In response, applicants respectfully state that although applicants do not agree with the equivalencies made in the office action between claim 3 and the cited reference, they indicate that claim 3 is dependent on allowable claim 1 and is allowable.

As per claim 4, Chari et al discloses of creating a randomized table includes applying a Table Split operation to at least one of said lookup tables resulting in split lookup tables (see page 404, section 3.3).

In response, applicants respectfully state that although applicants do not agree with the equivalencies made in the office action between claim 4 and the cited reference, they indicate that claim 4 is dependent on allowable claim 1 and is allowable.

As per claim 10, Chari et al teaches of the table is a table from a COMP128 application (see abstract and page 404, section 3.3).

In response, applicants respectfully state that although applicants do not agree with the equivalencies made in the office action between claim 10 and the cited reference, they indicate that claim 10 is ultimately dependent on allowable claim 1 and is allowable.

As per claim 11, it is disclosed by Chari et al of the number of elements in (be lookup table is given by a power of two (see page 404, section 3.3).

In response, applicants respectfully state that although applicants do not agree with the equivalencies made in the office action between claim 11 and the cited reference, they indicate that claim 11 is ultimately dependent on allowable claim 1 and is allowable.

As per claim 12, Chari et al teaches of employing said at least one randomized table in a cryptographic process, applying said at east one randomized table for securely handling information in said cryptographic process (see page 404, section 3.3).

Serial No.: 09/943,720

In response, applicants respectfully state that although applicants do not agree with the equivalencies made in the office action between claim 12 and the cited reference, they indicate that claim 12 is ultimately dependent on allowable claim 1 and is allowable.

As per claim 13, Chari et al discloses of prior to performing said cryptographic process, transforming the information by applying a secret-sharing operation to the elements of the information where each element of the information is related to multiple elements of the transformed information! performing the cryptographic process on the transformed information involving the use of said randomized table, and re-transforming the transformed and cryptographically processed information by applying an inverse secret-sharing operation to the transformed and cryptographically processed information (see page 404, section 3.3).

In response, applicants respectfully state that although applicants do not agree with the equivalencies made in the office action between claim 13 and the cited reference, they indicate that claim 13 is ultimately dependent on allowable claim 1 and is allowable.

As per claim 15, Chari at al teaches of employing data processing operation as a countermeasure against a first order side channel attack (see page 405, section 3.4).

In response, applicants respectfully state that although applicants do not agree with the equivalencies made in the office action between claim 15 and the cited reference, they indicate that claim 15 is ultimately dependent on allowable claim 1 and is allowable.

As per claim 18, it is disclosed by Chari et al that a table is a table from an application of General Countermeasures Against Side-Channel Attacks (see page 405, section 3.4).

In response, applicants respectfully state that although applicants do not agree with the equivalencies made in the office action between claim 18 and the cited reference, they indicate that claim 18 is ultimately dependent on allowable claim 1 and is allowable.

As per claim 29, it is disclosed by Chari et al of that the number of elements in the lookup table is 200 (see page 404, section 3,3).

In response, applicants respectfully state that although applicants do not agree with the equivalencies made in the office action between claim 29 and the cited reference, they indicate that claim 29 is ultimately dependent on allowable claim 1 and is allowable.

> *As per claim 30, Chari et al discloses of an article of manufacture comprising computer readable program code embodied thereon for causing resistance to side channel attacks that provides a data processing operation involving at least one lookup table, each particular table from said at least one lookup table having a particular lookup table size and a particular lookup table index size and creating at least one randomized table in which entries and/or indices are statistically independent from entries and/or indices of said at least one lookup table, each individual table from said at least one randomized table having a randomized table size, wherein a first sum of sizes of all said randomized tables is smaller than a second sum of sizes of all lookup tables, or the maximum index size of said randomized tables is less than the maximum index size of the lookup tables (see abstract; page 404, section 3.3; page 405, section 3.4).*

In response, applicants respectfully state that although applicants do not agree with the equivalencies made in the office action between claim 30 and the cited reference, they indicate that claim 30 is ultimately dependent on allowable claim 1 and is allowable.

> *As per claim 36, Chari et al teaches of a method comprising providing a data processing operation involving a first lookup table in a cryptographic process, said lookup table having a first lookup table size, creating a randomized table in which entries or indices are statistically independent of entries or indices of said first lookup table, said randomized table having a randomized table size being smaller than said first lookup table size, employing said randomized table for securely handling information in said cryptographic process prior to performing the cryptographic process, transforming the information by applying a secret-sharing operation to the elements of the information where each element of the information is related to multiple elements of the transformed information, performing the cryptographic process on the transformed information involving the use of said randomized table, and re-transforming the transformed and cryptographically processed information by applying an inverse secret. sharing operation to the transformed and cryptographically processed information (see page 404, section 3.3 and page 405, section 3.4).*

In response, applicants respectfully state that in order to bring the application to allowance claim 36 is amended to include the limitation of objected-to claim 7, which includes the limitations of claim 4. This makes claim 36 and all claims 37, 36 and 52, that depend on claim 36 to be allowable.

Serial No.: 09/943,720

As per claim 37, it is taught by Chari et al of using one randomized table (see page 404, section 3.3).

In response, applicants respectfully state that although applicants do not agree with the equivalencies made in the office action between claim 37 and the cited reference, they indicate that claim 37 is ultimately dependent on allowable claim 36 and is allowable.

As per claim 38, it is disclosed by Chari et al of the cryptographic process is performed in a cryptographic information processing system (see abstract).

In response, applicants respectfully state that although applicants do not agree with the equivalencies made in the office action between claim 38 and the cited reference, they indicate that claim 38 is ultimately dependent on allowable claim 36 and is allowable.

As per claim 39, Chariot et al discloses a chip card comprising a module for providing a data processing operation involving at least one lookup table, each particular table from said at least one lookup table having a particular lookup table size and a particular lookup table index size and creating at least one randomized table in which entries and/or indices are statistically independent from entries and/or indices of said at least one lookup table, each individual table from said at least one randomized table having a randomized table size, wherein a first sum of sizes of all said randomized tables is smaller than a second sum of sizes of all lookup tables, or the maximum index size of said randomized tables is less than the maximum index size of the lookup tables (see section 1, page 398 and page 404, section 3.3).

In response, applicants respectfully state that although applicants do not agree with the equivalencies made in the office action between claim 39 and the cited reference, they indicate that claim 39 is ultimately dependent on allowable claim 1 and is allowable.

As per claim 40, Chari at al teaches of a fixed lookup table (page 404, section 3.3).

In response, applicants respectfully state that although applicants do not agree with the equivalencies made in the office action between claim 40 and the cited reference, they indicate that claim 40 is ultimately dependent on allowable claim 1 and is allowable.

As per claim 41, it is disclosed by Chari et al of an apparatus for a randomizer module to create at least one randomized table in which entries and/or indices are statistically independent of entries; and/or indices of any table from a provided set of lookup tables, each individual table from said at least one randomized table having a randomized table size, wherein: a first sum of sizes of all said randomized tables is smaller than a second sum of sizes of all said at least one lookup tables, or the maximum index size of said randomized tables is less than the maximum index size of the lookup tables and a processing module to perform said data processing operation employing said first randomized table (page 404, section 3.3).

In response, applicants respectfully state that although applicants do not agree with the equivalencies made in the office action between claim 41 and the cited reference, they indicate that claim 41 is amended to include the limitations of objected-to claim 7, which includes the limitations of claim 4. This makes claim 41 and all claims 42-48, that depend on claim 41 to be allowable.

As per claim 42, Chad et al teaches that the randomized module forms the provided set of lookup tables (see page 404, section 3.3).

In response, applicants respectfully state that although applicants do not agree with the equivalencies made in the office action between claim 42 and the cited reference, they indicate that claim 42 is ultimately dependent on allowable claim 41 and is allowable.

As per claim 43, it is taught by Chad et al that the randomizer module includes a splitting module to perform a table split operation upon the subset of the set of lookup tables resulting in split lookup tables (see page 404, section 3.3).

In response, applicants respectfully state that although applicants do not agree with the equivalencies made in the office action between claim 43 and the cited reference, they indicate that claim 43 is ultimately dependent on allowable claim 41 and is allowable.

As per claim 52, Chari et al discloses of an article of manufacture comprising Computer readable program code embodied thereon for causing resistance to side channel attacks that provides a data processing operation involving a first lookup table in a cryptographic process, said lookup table having a first lookup table size, creating a randomized table in which entries or indices are statistically independent of entries or indices of said first lookup table, said randomized table having a randomized table size

being smaller than said first lookup table size, employing said randomized table for securely handling information in said cryptographic process prior to performing the cryptographic process, transforming the information by applying a secret-sharing operation to the elements of the information where each element of the information is related to multiple elements of the transformed information. performing the cryptographic process on the transformed information involving the use of said randomized table, and re-transforming the transformed and cryptographically processed information by applying an inverse secret-sharing operation to the transformed and cryptographically processed information (see abstract; page 404, section 3.3 and page 405, section 3.4).

In response, applicants respectfully state that although applicants do not agree with the equivalencies made in the office action between claim 52 and the cited reference, they indicate that claim 52 is ultimately dependent on allowable claim 36 and is allowable.

As per claim 53, Chari et al discloses of a program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine for causing resistance to side channel attacks that provides a data processing operation involving at least one lookup table, each particular table from said at least one lookup table having a particular lookup table size and a particular lookup table index size and creating at least one randomized table in which entries and/or indices are statistically independent from entries and/or indices of said at least one lookup table, each individual table from said at least one randomized table having a randomized table size, wherein a first sum of sizes of all said randomized tables is smaller than a second sum of sizes of all lookup tables, or the maximum index size of said randomized tables is less than the maximum index size of the lookup tables (see abstract; page 404, section 3.3; page 405, section 3.4).

In response, applicants respectfully state that although applicants do not agree with the equivalencies made in the office action between claim 52 and the cited reference, they indicate that claim 52 is ultimately dependent on allowable claim 1 and is allowable.

As per claim 55, Chari et al teaches of a program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine for causing resistance to side channel attacks that provides a data processing operation involving a first lookup table in a cryptographic process, said lookup table having a first lookup table size, creating a randomized table in which entries or indices are statistically independent of entries or indices of said first lookup table, said randomized table having a randomized table size being smaller than said first lookup table size, employing said randomized table for securely handling information in said cryptographic process prior to performing the cryptographic process, transforming the information by applying a

secret-sharing operation to the elements of the information where each element of the information is related to multiple elements of the transformed information, performing the cryptographic process on the transformed information involving the use of said randomized table, and re-transforming the transformed and cryptographically processed information by applying an inverse secret-sharing operation to the transformed and cryptographically processed information (see abstract; page 404. section 3.3; and page 405, section 3.4).

In response, applicants respectfully state that although applicants do not agree with the equivalencies made in the office action between claim 55 and the cited reference, they indicate that claim 55 is ultimately dependent on allowable claim 36 and is allowable.

As per claim 56, it is disclosed by Chari et al of a computer program product comprising a computer useable medium having computer readable program code embodied thereon for causing resistance to side channel attacks that provides a randomizer module to create at least one randomized table in which entries and/or indices are statistically independent of entries; and/or indices of any table from a provided set of lookup tables, each individual table from said at least one randomized table having a randomized table size, wherein: a first sum of sizes of all said randomized tables is smaller than a second sum of sizes of all said at least one lookup tables, or the maximum index size of said randomized tables is less than the maximum index size of the lookup tables; and a processing module to perform said data processing operation employing said first randomized table (see abstract; page 404, section 3.3; and page 405, section 3.4).

In response, applicants respectfully state that although applicants do not agree with the equivalencies made in the office action between claim 56 and the cited reference, they indicate that claim 56 is ultimately dependent on allowable claim 41 and is allowable.

Allowable Subject Matter

6. Claims 5-9, 14, 16, 17, and 44-48 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

In response, applicants respectfully state that objected-to claim 5 is incorporated into claim 1, and claim 5 is canceled. All objected-to claims 6-9, 14, 16, 17, and 44-48 are not dependent on

allowable claims and are also allowable. This overcomes the objection of objected-to claims 6-9, 14, 16, 17, and 44-48.

7. Claims 19-28, 31-35, 49-51, 54, and 57 are allowed.

In response, applicants respectfully state that appreciation for the allowance of claims 19-28, 31-35, 49-51, 54, and 57.

It is anticipated that this amendment brings the application to allowance of all claims 1-4, and 6-57. Favorable action is respectfully solicited. If any rejections or objections remain, please call the undersigned before issuing a FINAL action.

Please charge any fee other than the fee to revive, necessary to enter this paper to deposit account 50-0510. A credit card payment of the fee to revive, for $1500.00, is included on form PTO2038.

Respectfully submitted,

By: Louis Herzberg

Dr. Louis P. Herzberg
Reg. No. 41,500
Voice Tel. (845) 352-3194
Fax. (845) 352-3194

3 Cloverdale Lane
Monsey, NY 10952

Customer Number: 54856